

Coordinated Vulnerability Disclosure Policy

INOSIM GmbH

Document history

Version	Date	Description
V0.9	02.10.2026	Initial draft
V1.0	14.10.2026	First public release

Introduction

As a provider of products with digital elements, INOSIM GmbH is committed to ensuring the ongoing security of these products and to the security of our customers' production environments. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy defines how security researchers, customers, and the general public can report potential security vulnerabilities to us, and how we handle and disclose such reports in a coordinated manner and comply with the applicable obligations under the EU Cyber Resilience Act (Regulation (EU) 2024/2847), in particular Article 14 concerning the reporting of actively exploited vulnerabilities and severe incidents.

Scope

This policy applies to all INOSIM GmbH products with digital elements (hereinafter referred to as "products") made available on the market.

We accept vulnerability reports concerning all INOSIM GmbH products. The availability of security updates and mitigations depends on the applicable product support period and product lifecycle status.

Out of scope

- Vulnerabilities in third-party products or components that do not affect an INOSIM product or its components.
- Vulnerabilities found because of automated tools or scans without supporting documentation



How to report

If you believe you have discovered a security vulnerability, please report it to us as soon as possible by sending an Email to cert@inosim.com.

Please do not use public channels (forums, social media) to report active vulnerabilities before we have had a reasonable opportunity to investigate the issue and coordinate disclosure.

For secure, encrypted communications, please use our OpenPGP Public Key available for direct download at <https://www.inosim.com/.well-known/cert-pgp.asc>. We accept anonymous submissions.

While anonymous reporting may limit our ability to clarify technical details with you, we will fully investigate all credible reports regardless of the reporter's anonymity.

You can report in English or German.

Information to include

Please include as much of the following as possible:

- A description of the vulnerability and its potential impact (e.g. remote code execution, privilege escalation, denial of service, data leakage).
- Specific product and version (e.g. INOSIM2026 16.0.10) and affected component
- Any assigned CVE ID (Common Vulnerabilities and Exposures), if applicable.
- Steps to reproduce the issue or proof-of-concept code.
- Any relevant screenshots.
- Affected configurations and dependencies (e.g. OS)
- Suggested mitigation or fix, if you have one.
- Your contact information for follow-up, preferable via Email or Telephone.

Our handling process

Upon receiving your report, we will:

- Acknowledge receipt of your report, within 5 business days, unless a vulnerability was reported anonymously. Reports determined to be spam or out-of-scope will be closed immediately without further acknowledgment or response.
- Detailed feedback after further analysis is provided within 10 business days, unless a vulnerability was reported anonymously.
- We may contact you during the investigation to gather additional technical details and/or to understand and validate the issue.
- Strive to resolve the vulnerability promptly.
- Ensure that all reports are analyzed and processed thoroughly
- Keep you informed, as appropriate and practicable, of significant progress and expected timelines throughout the CVD process.
- Where applicable, we will fulfil the reporting and user notification obligations established by Article 14 of the EU Cyber Resilience Act within the required timeframes.

The CVD process will be completed once a remediation solution has been made available (and, where applicable, the vulnerability is publicly disclosed), or if the reported vulnerability has



been determined to be unfounded.

Coordinated disclosure timeline

As a general guideline, we aim to coordinate disclosure within 90 days of receiving a report. The actual timeline may be adjusted depending on the severity of the vulnerability, the availability of a fix or mitigation, the risk to affected users, and applicable legal requirements. We will coordinate the disclosure timeline with the reporter where reasonably possible.

Where required, we will inform affected users without undue delay and provide available mitigation or corrective measures.

Safe Harbor

INOSIM GmbH will not initiate legal action against any researcher who discovers and reports vulnerabilities in our products in good faith and gives us a reasonable opportunity to remediate the issue.

Changes to this policy

This policy may be updated from time to time and reviewed at least once a year.

Security contact

Our Security Incident Response Team can be contacted via: cert@inosim.com.

We publish a security.txt file at <https://www.inosim.com/.well-known/security.txt> so that automated tools and researchers can discover our security contact information.